

Microsoft’s Response to Request for Comment
Department of Commerce, National Telecommunications and Information Administration

The Benefits, Challenges, and Potential Roles for Government in Fostering the Advancement of the Internet of Things

I. Introduction

Microsoft Corporation (“Microsoft”) appreciates the opportunity to provide comments to the U.S. Department of Commerce (“Commerce”) and specifically the National Telecommunications and Information Administration (“NTIA”) in response to its renewed request for comments on the benefits, challenges, and potential roles for the government in fostering the advancement of the Internet of Things (“IoT”).

As a global technology company, Microsoft is a provider of the hardware, software, and cloud services that power IoT. We help our customers connect, monitor, and manage millions of devices and related assets, and we provide the cloud services that help organizations unlock the value of new business models that are possible only through the combination of connected devices, machine learning, and big data analytics that power IoT. This diversity of offerings gives us a unique—and, we believe, uniquely balanced—perspective on IoT issues.

Microsoft commends NTIA for its January 12, 2017, green paper, *Fostering the Advancement of the Internet of Things* (the “green paper”). Microsoft is encouraged by the green paper, which aligns with many of Microsoft’s prior comments on encouraging the development and adoption of IoT technologies. In particular, Microsoft appreciates Commerce’s recognition that IoT represents a collection of a wide variety of new technologies that defy a single definition, and the challenges associated with the ubiquitous distribution and interconnectivity of these new technologies and devices. We also share Commerce’s view that the policy (and particularly security) issues raised by IoT are best addressed through flexible, risk-based solutions rather than fixed, prescriptive requirements.

Microsoft is concerned, though, by Commerce’s recommendations for patching of discontinued products. Microsoft agrees with Commerce that “orphaned devices” (connected devices that are no longer supported by their manufacturer) can contribute to the threat landscape. However, Microsoft believes that software and device upgrades can often enable better protections than patching old products that simply should be taken offline. In addition, encouraging the continued use of older devices may create insecurities and other unintended problems, particularly as the network supporting those devices evolves based on newer technologies.

Relatedly, Microsoft further agrees that IoT users should have the option to utilize encryption at the device, application, and network layers, depending on the user’s risk assessment and security preferences. At the same time, many users may not be well-served when faced with the prospect of managing encrypted data and devices. Commerce should consider these nuances as it proceeds with its initiatives related to IoT security.

II. IoT Landscape

The green paper appreciates that IoT is different from prior technological changes our society has faced in a number of important respects.¹ *First*, IoT has a wider scope than prior technological developments, because it directly connects a broader range of systems and devices and thus requires new forms of cross-sector and public-private collaboration. *Second*, IoT presents these issues on a much greater scale than prior technological changes; the sheer number of future IoT endpoints will present new infrastructure challenges, including capacity, resilience, and related public policy issues. *Third*, the stakes are higher with IoT than with prior technological advances, because IoT deployments are often characterized by the intersection of information technology (“IT”) and operational technology (“OT”). Microsoft agrees with the green paper’s assessment of these important differences and recognizes that the technological evolution away from notions of traditional computer networks and hosts, and toward the direct interconnectedness of everyday objects in the physical world represents a paradigm shift in the way we live.²

Microsoft also endorses the green paper’s “broad, flexible approach to the definition of IoT,” particularly at this juncture.³ As the green paper recognizes, Microsoft’s prior comments urged Commerce to avoid “defining IoT narrowly, in a manner that may limit the scope of its potential applications” and instead to “recogniz[e] that the term IoT does not simply describe a new type of technical architecture, but a new concept that defines how we interact with the physical world.”⁴ The green paper therefore commits to using IoT as an “umbrella term,” but observes that when a “consensus technical definition may facilitate policy development” Commerce will consider “narrowly tailoring its policy inquiries and actions around categories of uses and/or devices rather than on all of IoT.”⁵ This use of the term thus embraces the view of IoT as a collection of specific categories of technology, rather than as a single unified subject.⁶

The green paper also reflects considered thought on the role of government in fostering IoT, both domestically and internationally. Domestically, it recognizes the need to avoid over regulation of IoT because of the notable risk of premature and excessive regulation of technology, particularly in its nascent stages, that carries great potential economic benefits to U.S. producers and consumers.⁷ At the same time, the green paper defers to future policy makers to determine the value of crafting a national strategy.⁸

Microsoft urges Commerce to consider the creation of a federal interagency task force that can coordinate with existing organizational bodies to foster balanced perspectives on security,

¹ See Department of Commerce Internet Policy Task Force & Digital Economy Leadership Team, *Fostering the Advancement of the Internet of Things*, January 2017 (“Green paper”) at 3.

² See Microsoft’s Response to Request for Comment on the Benefits, Challenges, and Potential Roles for Government in Fostering the Advancement of the Internet of Things, June 2, 2016 (“Microsoft Comments”), at 2-3.

³ Green paper at 7.

⁴ *Id.*

⁵ *Id.*

⁶ *Id.*

⁷ *Id.* at 11.

⁸ *Id.* at 10.

(continued...)

economic benefits, and potential risks. Such a task force, recommended in Microsoft’s prior comments, would also be in line with the government’s encouragement of multistakeholder approaches and private sector coordination and leadership where possible.⁹

Internationally, the green paper recognizes the need for the U.S. government to continue advocating for industry-led approaches and consensus-based standards.¹⁰ In particular, Microsoft encourages Commerce to use existing government-to-government dialogues to counter potential barriers to cross-border data flows, tariff and nontariff barriers to trade in goods, weak protections for intellectual property, and discriminatory practices that favor state-owned enterprises. These practices may particularly harm IoT because they have the potential not only to unnecessarily restrict the growth of IoT, but also to limit its benefits by encouraging regional markets for IoT rather than supporting the development of global technologies.

III. Areas of Engagement

The green paper identifies four broad areas for Commerce’s engagement with stakeholders on IoT: (1) enabling infrastructure availability and access, (2) crafting balanced policy and building coalitions, (3) promoting standards and technology advancement, and (4) encouraging markets.¹¹

A. Enabling Infrastructure Availability and Access

The first area of engagement is fostering the physical and spectrum-related assets needed to support IoT growth and advancement. The sheer increase in the number of connected devices associated with IoT will stress existing infrastructure, including both legacy networks and more recently-developed Internet Protocol (“IP”) systems.¹²

Four areas of specific concerns are identified: (1) the need for modernization of legacy communications infrastructure and the build out of additional broadband-capable networks, (2) an increased demand for spectrum amid a potential shortage of available spectrum, (3) the need for more Internet Protocol (“IP”) addresses, which could be mitigated by a transition from IPv4 to IPv6, and (4) issues of equity that may arise when underserved communities lack connectivity and could therefore be prevented from realizing the benefits of IoT.¹³

Microsoft agrees with the green paper’s assessment that the push for infrastructure deployment and development should be private-sector led.¹⁴ Microsoft also encourages Commerce to continue its activities in support of IPv6 adoption, which will be an important element in addressing the infrastructure stressors that accompany increased connectivity.

⁹ Microsoft Comments at 2, 17-18; Green paper at 11.

¹⁰ Green paper at 12-13.

¹¹ *Id.* at 15.

¹² *Id.* at 16-19.

¹³ *Id.* at 16-20.

¹⁴ *Id.* at 21.

(continued...)

B. Crafting Balanced Policy and Building Coalitions

The second area of engagement is creating balanced policy and building coalitions by removing barriers and encouraging coordination and collaboration. This involves influencing, analyzing, devising and promoting norms and practices that will protect IoT users while encouraging the growth, advancement, and applicability of IoT technologies.¹⁵ The green paper identifies four subject areas in which these policy efforts will focus: (1) cybersecurity, (2) privacy, (3) intellectual property, and (4) the free flow of data across borders.

Microsoft supports coordinated engagement in these policy areas to build forward-looking policies. Still, Microsoft is concerned that the green paper's treatment of a small number of issues in the cybersecurity realm may not advance the paper's goal of achieving balanced policies. In particular, the discussions of security patching and encryption could be read as favoring mandates, rather than flexible solutions that could help to overcome some of the technical complexities associated with encryption and patching on this scale. Microsoft believes Commerce should revisit these discussions in order to ensure the agency pursues balanced policies across all subject areas, and does not inadvertently hamper other key goals to foster the growth of IoT, including ensuring data integrity and availability.

1. *Cybersecurity*

Microsoft agrees with the green paper's assessment that "[j]ust as there is no easy description for IoT itself, there is no single prescription for IoT security."¹⁶ The discussions of security patching and encryption, however, veer from this general guidance and instead suggest measures that are ill-suited to the wide range of IoT technologies and the complexity of ubiquitous interconnectedness.

Because each element of the IoT ecosystem has the potential to introduce new and different security risks, there is a need to look not for standardized solutions but to security measures that reflect actors' roles in the IoT ecosystem. Indeed, as described in Microsoft's initial comments, there are different security practices appropriate for the roles of manufacturers/integrators, developers, deployers, and operators of IoT.¹⁷ These practices reflect not only Microsoft's experience in the IoT ecosystem, but also our recognition that a holistic approach to security requires consideration of role-based contributions from participants.

a) Patching

A number of commenters recognized that the lifespan of IoT devices will vary from short periods of time to many years.¹⁸ Taking these comments into account, Commerce opined that, "[t]he threat posed by orphan devices – devices no longer supported by their manufacturers – must also be addressed. Devices that consumers continue to use to connect to the Internet should be updated and protected even if device manufacturers discontinue them. There should be some

¹⁵ *Id.* at 3, 24.

¹⁶ *Id.* at 26.

¹⁷ Microsoft Comments at 7-10.

¹⁸ Green paper at 28-29.

(continued...)

mechanism (such as transferring the needed software keys to a designated consortium) for ensuring that devices function with the software updates needed to ensure security.”¹⁹

Microsoft is concerned that Commerce’s statement could be read as effectively calling for unlimited support for connected devices, which would have a number of problematic implications. Certain security advancements (e.g., hardware-based roots of trust) are only enabled through new hardware and are not addressed simply by patching. In addition, as developments in biometrics and other authentication mechanisms advance, new security features cannot always be added by patching, and continued use of older features may result in unintended consequences across the network of newer technologies. In many cases, then, continuously patching old software or firmware produces less secure outcomes.

Commerce should give careful consideration to the implications of unlimited patching of discontinued technology products, including the business costs. Unlimited support would likely stifle innovation by putting a high cost burden on market entrants, thereby providing a disincentive to consumers to upgrade their old technology due to cost, as well as a mistaken belief that their older products are inherently as secure as newer devices. In addition, Microsoft also urges Commerce to acknowledge that basic cyber hygiene is still a critical concern; many responsible technology providers ship patches on a regular basis, but users often fail to apply them.

Microsoft is also concerned by Commerce’s statement contemplating use of a consortium-type body to manage software updates and/or the underlying source code to handle orphaned devices.²⁰ Inserting a new third-party between the technology provider and its users would create a new attack vector and may just make it more difficult and less efficient to produce good patches. Patching can be a complex process for organizations even when they are working with their own code. Moreover, technology companies are unlikely to embrace a model in which their code is handed over to a third party; source code is a significant corporate asset.

In contrast, encouraging IoT manufacturers and developers to consider updatability more broadly—including not just patching but also through upgrading products with new security technologies that address evolving security threats—would ensure that all IoT devices address continued security needs in appropriate ways.

b) Encryption

Commenters recognized the use of encryption may increase security for a number of IoT devices.²¹ Based in part on these comments, Commerce articulated its intent to “promote the use of strong encryption in IoT services and products to address security concerns in the government’s risk-based approach to the use and application of IoT technologies.”²²

Commerce’s comments about encryption present some risk of an unmanageable requirement on the wide array of technologies that compose the IoT landscape, potentially at the cost of data

¹⁹ *Id.* at 41.

²⁰ *Id.*

²¹ *Id.* at 30.

²² *Id.* at 57.

availability. For example, data encryption comes with its own challenges and potential downsides, such as effective key management and loss of access to and potential processing of data. This is often a challenging proposition even for enterprise technology users.

Microsoft uses encryption broadly across its cloud services, but we also provide users with encryption choices for some aspects of their cloud deployments.²³ This approach empowers users to make decisions about encryption commensurate with their risk profile, deployment characteristics, and other factors that are unique to the sensitivity of the data they store and the purposes for which the data is used. Indeed, encryption is appropriate in many instances and particularly where important data may be involved. However, users that elect to encrypt their data may not be able to leverage certain value-added services, such as automated malware scanning and other processing capabilities, because encryption may prevent the scanner from reviewing the underlying code. These tradeoffs are relevant to a user's individual choice whether to encrypt data.²⁴

Microsoft therefore urges Commerce to take a more nuanced approach to the use of encryption in IoT. There will be scenarios in which encryption at the device, application, and network layers will be a key tool in securing an IoT deployment. However, there are other scenarios, particularly at the consumer level, in which users will not need or want to use encryption. Users should be allowed to weigh these tradeoffs and to make choices that are appropriate for each of their IoT devices.

2. *Privacy*

Given the variety of IoT devices, the green paper recognizes that “connected devices are not all equal in their relative effects on privacy.”²⁵ Microsoft believes that strong data protection frameworks reflect the core principle of technology neutrality by focusing on principles and outcomes, rather than imposing prescriptive requirements.

Microsoft also endorses Commerce's support of baseline privacy legislation, which could address privacy concerns without regard to the type of technology used. One of the most significant barriers to adoption of new technologies such as IoT is a lack of consumer trust. When consumers know their privacy is protected by robust laws, though, they will adapt to new innovations like IoT with greater confidence. Microsoft has long supported baseline privacy legislation—and robust enforcement for those that breach standards created by such legislation—

²³ See Microsoft, *Protecting Customer Data from Government Snooping*, Dec. 4, 2013, available at <https://blogs.microsoft.com/blog/2013/12/04/protecting-customer-data-from-government-snooping/>; Microsoft, *Advancing our encryption and transparency efforts*, July 1, 2014, available at: <https://blogs.microsoft.com/on-the-issues/2014/07/01/advancing-our-encryption-and-transparency-efforts/>.

²⁴ For example, an IoT system may have encryption at different layers, and each layer can protect against its own class of threat. Encryption at the transport layer can be very important, as it mitigates threats to data exchanged on the wire, an obvious attack surface. Going up the stack, encryption of each data element before it is put on the transport layer may be helpful since it can impact operations. Going further up the stack, one could encrypt data at rest (in the cloud or on a gateway), which may still be worthwhile in certain use cases. The choice needs to be with the user.

²⁵ Green paper at 30.

(continued...)

for this reason. Modernizing privacy frameworks for IoT to ensure strong privacy protections will help foster the advancement of IoT.²⁶

3. *Intellectual Property*

IoT also raises novel questions of intellectual property. In the field of copyright, the extent to which data outputs produced by IoT devices will include copyrightable sounds or images, or will reflect a sufficiently original selection or presentation of data that is entitled to protection under copyright laws is still developing.²⁷ In patent law, intellectual property rights are expected to play a key role in developing IoT, by providing incentives to innovators to develop better IoT devices, manufacturing practices, and infrastructure.²⁸ Trade secrets laws may pose similar incentives, particularly by protecting algorithms associated with IoT technologies.²⁹ Trademarks may also serve as quality indicators or indicate certifications that goods meet certain standards for interoperability.³⁰ While few of these issues are unique to IoT, Microsoft supports Commerce’s goal of continuing to promote the positive evolution of intellectual property and its protection in the digital economy.³¹

4. *Free Flow of Data Across Borders*

Because a free and open global internet is the “lynchpin of the digital economy,” the green paper recognizes the importance of minimizing barriers to the flow of information and services across national borders.³² As commenters emphasized, policies that limit cross-border data flows can negatively affect the growth of IoT sectors by impeding the normal functioning of the devices, as many IoT devices are designed to frequently cross borders. Such policies also raises costs, especially for small and medium-sized companies, slowing their economic growth.³³ For IoT technologies to thrive, data must be able to flow not only between IoT devices, but in many cases back to the cloud platform that hosts the network running those devices.

Microsoft supports the green paper’s proposal that Commerce continue to work with international partners toward an industry-led global marketplace that supports free flow of information.³⁴ As the paper recognizes, this would further the ability of American companies to compete fairly around the world and promote innovation.³⁵

Microsoft encourages Commerce to consider the full range of forums available to advance these goals. As noted in our earlier input, Commerce should leverage multilateral and bilateral trade agreements to advance the global IoT marketplace.³⁶ For example, World Trade Organization (“WTO”) agreements contain binding rules and commitments relevant to IoT, including all the

²⁶ Microsoft Comments at 11.

²⁷ Green paper at 34-35.

²⁸ *Id.* at 36.

²⁹ *Id.* at 38.

³⁰ *Id.* at 39.

³¹ *Id.* at 42.

³² *Id.* at 39.

³³ *Id.* at 40.

³⁴ *Id.* at 44.

³⁵ *Id.*

³⁶ Microsoft Comments at 16.

goods-related agreements (in particular provisions related to standards), such as the General Agreement on Trade in Services (“GATS”); the Agreement on Trade-Related Aspects of Intellectual Property Rights (“TRIPS”); and the plurilateral WTO Information Technology Agreement (“ITA”), which eliminates tariffs on many high technology goods. Commerce should serve as an advocate for IoT-related dialogue in these venues, alongside interagency partners that have roles in trade matters.

C. Promoting Standards and Technology Advancement

The third area of engagement is promoting standards and technology advancement by ensuring that technical standards are developed and implemented to support global IoT interoperability.³⁷ As the green paper recognizes, a wide range of standards addressing different aspects of IoT applications, including technology, connectivity, interoperability, functionality, security, and usability will be needed.³⁸

Microsoft agrees with Commerce’s conclusion that “[i]ndustry, with active participation from government experts as needed, is ideally positioned to lead the development of technological standards and solutions to address global IoT environment opportunities and challenges.³⁹ Further, Microsoft shares the belief that because the “vast and expansive nature of the technologies underpinning IoT, no single standards developing organization has the resources or the expertise to develop all of the standards that will be needed.”⁴⁰

Commerce’s goal of “continu[ing] to support IoT standards development that is bottom-up and private-sector led”⁴¹ aligns with Microsoft’s prior comments. Because collaboration with industry is key to the development of any new IoT standards, the development of open, voluntary, consensus-based, and globally-relevant standards is a major driver of a robust and competitive IoT marketplace.⁴²

D. Encouraging Markets

The fourth area of engagement is promoting the advancement of IoT through Commerce’s own usage, application, and iterative enhancement of the technology.⁴³ As the green paper recognizes, the U.S. government as a whole and Commerce in particular can encourage the development and growth of IoT devices by being a leading consumer and adopter of IoT.⁴⁴

The green paper also endorses the type of public-private partnerships that Microsoft has long supported, by recognizing that the public sector can be a leading adopter of emerging technologies. For example, Microsoft has developed a seven-step approach to help cities design

³⁷ Green paper at 3, 44.

³⁸ *Id.* at 44.

³⁹ *Id.* at 45.

⁴⁰ *Id.* at 46.

⁴¹ *Id.* at 47.

⁴² Microsoft Comments at 11.

⁴³ Green paper at 3, 49.

⁴⁴ Green paper at 49.

(continued...)

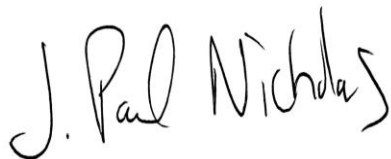
and implement cybersecurity strategies⁴⁵ and has partnered with 100 Resilient Cities to help cities improve their digital resiliency capabilities.⁴⁶

In addition to fostering such partnerships, though, Microsoft encourages Commerce to take the further step of supporting the creation of an interagency task force dedicated to IoT. Such a task force would coordinate with existing organizational bodies to foster balanced perspectives between security, economic benefits, and potential risks, and to incentivize market participation. The task force could include a number of federal government agencies, and could direct the update of federal strategic documents addressing IoT growth and resilience, awareness and training programs, and encourage the development of academic curricula focused on IoT, as detailed in Microsoft's prior comments.⁴⁷

IV. Conclusion

Microsoft appreciates the opportunity to provide these further comments to assist the NTIA and Commerce in considering the benefits, challenges, and potential roles for government in fostering the advancement of IoT. Microsoft encourages Commerce to continue its work in advancing the development of IoT technologies and related policies and would welcome the opportunity to work with NTIA and Commerce in considering how best to address the benefits and challenges of IoT in the future.

Sincerely,



J. Paul Nicholas
Senior Director
Trustworthy Computing
Microsoft Corporation

⁴⁵ See Microsoft, *Developing a City Strategy for Cybersecurity*, July 2014, available at <http://az370354.vo.msecnd.net/publicsector/citynext/whitepapers/Developing%20City%20Strategy%20for%20CyberSecurity.pdf>.

⁴⁶ See Microsoft, *100 Resilient Cities and Microsoft Partner to Build City Cybersecurity Strategies*, Jan. 15, 2015, available at <https://www.microsoft.com/en-us/citynext/blogs/100-resilient-cities-and-microsoft-partner-to-build-city-cybersecurity-strategies/default.aspx>.

⁴⁷ Microsoft Comments at 17.